(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 881 665 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
**29.12.2010 Bulletin 2010/52**

(21) Application number: **06117582.4**

(22) Date of filing: **20.07.2006**

(51) Int Cl.:
***H04L 29/06*** *(2006.01)* ***H04L 12/22*** *(2006.01)*

(54) **System and method for provisioning device certificates**

Vorrichtung und Verfahren zur Versorgung von Apparatzertifikaten

Système et méthode pour fournir des certificats d'appareil

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR**
Designated Extension States:
**AL BA HR MK RS**

(43) Date of publication of application:
**23.01.2008 Bulletin 2008/04**

(60) Divisional application:
**10175746.6 / 2 254 304**

(73) Proprietor: **RESEARCH IN MOTION LIMITED**
**Waterloo, Ontario N2L 3W8 (CA)**

(72) Inventors:
- **Brown, Michael K**
  **Kitchener, Ontario N2M 2Z2 (CA)**
- **Brown, Michael S**
  **Waterloo, Ontario N2K 4B1 (CA)**
- **Kirkup, Michael G.**
  **Waterloo, Ontario N2J 4Y3 (CA)**

(74) Representative: **Patel, Binesh et al**
**Barker Brettell LLP**
**10-12 Priests Bridge**
**London**
**SW15 5JE (GB)**

(56) References cited:
**US-A1- 2005 154 795** **US-A1- 2005 287 990**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 881 665 B1

Printed by Jouve, 75001 PARIS (FR)

## Description

**[0001]** The present invention relates generally to digital security and specifically to a system and method for provisioning device certificates.

**[0002]** The continued growth of telecommunication networks has led to the proliferation of communication devices that are used for the transfer of both voice and data. Personal Digital Assistants (PDAs) and smart-phones are examples of wireless communication devices that enable users to communicate via voice communications, electronic mail (e-mail), Short Message Service (SMS) messages as well as instant messaging. Additionally, many of these devices also include Web browsers and other applications to provide the users with information and access to remote data.

**[0003]** Due to their portability and ever-increasing functionality, wireless communication devices are becoming a necessity in today's business environment. Conducting business on the Internet is often efficient and cost effective, particularly when products and services can be distributed electronically.

**[0004]** However, as more people have access to the network and more data becomes available on the network, the risk of the wrong people accessing sensitive data increases. Accordingly, it is desirable for many network administrators to limit the devices that can access their network. One mechanism for limiting such access is the use of device certificates.

**[0005]** A device certificate is defined as a public key certificate or an attribute certificate tying the identity of a device to its attributes. An example of the use of digital certificates is the Device Certificate Service provided by VeriSign®. The VeriSign® Device Certificate Service embeds X.509 certificates into hardware devices, which allows service providers to perform strong authentication of their devices. Device manufacturers order certificates in bulk by providing a list of Media Access-Control (MAC) addresses or unique device identifiers for the certificates. The issued certificates are returned to the manufacturers, who can then incorporate the process of injecting the certificates into the target devices as part of its overall device manufacturing process.

**[0006]** However, the process of assigning digital certificates during manufacture places an unnecessary burden on the manufacturing process. Further, it limits the digital certificate to a single certifying authority, regardless of the device's purchaser.

**[0007]** U.S. Patent Application No. 11/002,315 filed by Tet Hin Yeap et al and titled "System and Method for Access Control" teaches a system for restricting access based on device certificates. In order to assign a certificate to a device, Yeap teaches a system administrator transmitting an email request. The email includes unique identifiers of both the device and an access server. Both identifiers are used to generate a certificate, which is transmitted to the device via an email.

**[0008]** US2005/0287990 discloses a method tor issuing certificates which are bound to users only, and which can thus be transferred betWeen' different user devices.

**[0009]** However, the use of the access server identifier ties the device to a single access server. Further, the method requires an email from a system administrator to initiate the certificate. For application in less technically sophisticated companies, such a step would provide an unnecessary burden on the user.

**[0010]** Lastly, in a document titled "Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2: Appendix A. Deploying Exchange ActiveSync with Certificate-Based Authentication" a method for certificate enrolment configuration is taught. The document teaches a system administrator configuring an Extensible Markup Language (XML) script for device certificate enrolment. The XML script is uploaded to Active Directory using Microsoft Visual Basic Scripting Edition (VBScript). Active Directory is a Microsoft® directory service provided by a network server that provides means to manage identities and relationships that make up a network environment. Accordingly, when a user "cradles" a device, it connects to a corporate network via software on the user's computer. At this point, the XML script created by the administrator is delivered to the device and the certificate enrolment can begin.

**[0011]** However, similar to the previously described solution, the solution presented by this document is difficult to implement. Further, it requires that the device be able to communicate with a server via a cradle arrangement. Such a set-up precludes wireless certificate registration.

**[0012]** Accordingly, there is a need for a method of provisioning device certificates that overcomes the limitations of the prior art.

GENERAL

**[0013]** A certificate creation request is preferably bootstrapped on to an activation process and generated by the device itself. During this process, the device preferably creates a certificate request in the form of a certificate service request. This certificate service request preferably includes both a device identifier and a corresponding user's identifier to bind the two together.

**[0014]** In accordance with one embodiment there is preferably provided a method for provisioning a device certificate on a device configured to communicate wirelessly with a plurality of backend servers via a communication network including a mobile data server, the method comprising the steps of: initiating an activation request to the mobile data

server for activating the device on the communication network; during activation of the device, providing a device certificate request to the mobile data server for the device, the device certificate request including at lease a user identifier, a device identifier and a device public key, wherein the device certificate request is forwarded from the mobile data server to a predefined certification authority; and receiving a device certificate from the predefined certification authority in response to the device certificate request.

[0013a] In accordance with another embodiment there is preferably provided a method for provisioning a device certificate on a device configured to communicate wirelessly with a plurality of backend servers via a communication network comprising a mobile data server, the method comprising the steps of: receiving an activation request at the mobile data server for activating the device on the communication network; during activation of the device, receiving a device certificate request at the mobile data server for the device, the device certificate request comprising at least a user identifier, a device identifier and a device public key; and forwarding the device certificate request from the mobile data server to a predefined certification authority, wherein a device certificate is forwarded from the predefined certification authority to the device in response to the device certificate request.

**[0015]** In accordance a further embodiment there is preferably provided a wireless communication device comprising: means for initiating an activation request to a mobile data server for activating the device on a communication network; means for providing a device certificate request to the mobile data server for the device during activation of the device, the device certificate request comprising at least a user identifier, a device identifier and a device public key, wherein the device certificate request is forwarded from the mobile data server to a predefined certification authority; and means for receiving a device certificate from the predefined certification authority in response to the device certificate request.

[0014a] In accordance with another embodiment there is preferably provided a computer program product for provisioning a device certificate on a device configured to communicate wirelessly with a plurality ofbackend servers via a communication network having a mobile data server, the computer program product comprising instructions which, when executed on a processor of the device, cause the device to implement either of the methods described above.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0016]** Embodiments of the present invention will now be described by way of example only with reference to the following drawings in which:

**Figure 1** is a block diagram illustrating a communication network infrastructure;
**Figure 2** is a flow chart illustrating a device provisioning process; and
**Figure 3** is a block diagram illustrating a mobile device.

## DESCRIPTION OF PREFERRED EMBODIMENTS

**[0017]** For convenience, like numerals in the description refer to like structures in the drawings. Referring to Figure 1, a communication network infrastructure for a wireless communication device is illustrated generally by numeral 100. The communication infrastructure 100 comprises a plurality of communication devices 102, or simply devices 102, a communication network 104, , a certification authority (CA) 118 and a plurality of backend servers 108.

**[0018]** The devices 102 include wireless computing devices such as a smart phone, a personal digital assistant (PDA), and the like. The devices 102 are in communication with one or more of the backend servers 108 via the communication network 104. Accordingly, the communication network 104 may include several components such as a wireless network 110, a relay 112, a corporate server 114 and/or a mobile data server 116 for relaying data between the devices 102 and the backend servers 108. An example of a mobile data server 116 is the BlackBerry Enterprise Server provided by Research in Motion.

**[0019]** The backend servers 108 include servers such as a Web server 108a, an application server 108b, and an application server with web services. It will be appreciated by a person of ordinary skill in the art that the network architecture described herein is exemplary and that changes may be made to one or more components to accommodate different network configurations without affecting the scope of the invention described and claimed herein.

**[0020]** Referring to Figure 3, a typical device 102 is illustrated in more detail. The device 102 is often a two-way communication device having both voice and data communication capabilities, including the capability to communicate with other computer systems. Depending on the functionality provided by the device mobile, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device such as a PDA (with or without telephony capabilities).

**[0021]** The device 102 includes a communication subsystem 311, which includes a receiver 312, a transmitter 314, and associated components, such as one or more embedded or internal antenna elements 316 and 318, local oscillators (LOs) 313, and a processing module such as a digital signal processor (DSP) 320. As will be apparent to those skilled in field of communications, the particular design of the communication subsystem 311 depends on the communication

network in which device 102 is intended to operate.

**[0022]** The device 102 includes a microprocessor 338 which controls general operation of the device 102. The microprocessor 338 also interacts with additional device subsystems such as a display 322, a flash memory 324, a random access memory (RAM) 326, auxiliary input/output (I/O) subsystems 328, a serial port 330, a keyboard 332, a speaker 334, a microphone 336, a short-range communications subsystem 340 such as Bluetooth™ for example, and any other device subsystems or peripheral devices generally designated at 342. Operating system software used by the microprocessor 338 is preferably stored in a persistent store such as the flash memory 324, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 326.

**[0023]** The microprocessor 338, in addition to its operating system functions, preferably enables execution of software applications on the device 102. A predetermined set of applications, which control basic device operations, is installed on the device 102 during its manufacture. These basic operations typically include data and voice communication applications, for example. Additionally, applications may also be loaded onto the device 102 through the communication network 104, an auxiliary I/O subsystem 328, serial port 330, short-range communications subsystem 340, or any other suitable subsystem 342, and installed by a user in RAM 326 or preferably a non-volatile store (not shown) for execution by the microprocessor 338. Such flexibility in application installation increases the functionality of the device 102 and may provide enhanced on-device features, communication-related features, or both.

**[0024]** The display 322 is used to visually present an application's graphical user interface (GUI) to the user. The user can manipulate application data by modifying information on the GUI using an input device such as the keyboard 332 for example. Depending on the type of device 102, the user may have access to other types of input devices, such as, for example, a scroll wheel, light pen or touch sensitive screen.

**[0025]** Before the user can use the device 102 to access the backend servers 108, an activation process registers the device 102 with the communication network 104. The activation process is an application executing on the device. The activation process may be part of the device operating system or an addition thereto. Referring to Figure 2, a flow diagram illustrating the activation process is illustrated generally by numeral 200.

**[0026]** In step 202, the activation process is initiated. In the present embodiment, the activation process is initiated by the user selecting an activation program on the device 102. However it will be appreciated that the activation process could be initiated by the device 102 itself upon startup or at a predetermined time, for example. Furthermore, the activation process could be initiated by the user via a website using a pre-existing network connection, such as using a personal computer with Internet access for example.

**[0027]** Once the activation process is initiated, it continues at step 204. In step 204, the user is prompted to enter user identification. In the present embodiment, the user identification includes a pre-assigned electronic mail (email) address and an activation password. The activation password is established by a system administrator for the purpose of the activation process. In the present embodiment, the system administrator can be either a corporate Information Technology (IT) department or a service provider, depending on the implementation selected by the user.

**[0028]** In step 206, the device 102 transmits an activation request message to the mobile data server 116. The activation request message includes information about the device 102, such as routing information and the device's activation public keys, for example. In the present embodiment, this is achieved by transmitting an activation request email to the user's email account. The mobile data server 116 receives the activation request email en route and retrieves the information.

**[0029]** In step 208, the mobile data server 116 sends an activation response message to the device 102. The activation response message includes information about the mobile data server 116 such as routing information and the mobile data server's public keys, for example. In the present embodiment, this is achieved by transmitting an activation request email that is received by the device 102.

**[0030]** In step 210, the mobile data server 116 and the device 102 establish a master encryption key. Both the mobile data server 116 and the device 102 verify their knowledge of the master encryption key to each other. Generation and verification of such a master encryption key is beyond the scope of the present invention and it will be appreciated that any appropriate state-of-the-art or proprietary technique may be used.

**[0031]** One such technique is described in detail in Applicant's co-pending U.S. Application Serial No. 11/093,954, titled "Deploying and Provisioning Wireless Handheld Devices", and filed March 30, 2005. Using this technique, the user generates a long-term encryption key pair and a short-term authentication key pair. The authentication key pair is generated using a shared secret. In the present embodiment, the shared secret is the activation password. The public keys of both key pairs are used as the activation public keys.

**[0032]** Once the device's public keys are received by the mobile data server 116, the user is verified. Once the device 102 is verified, the mobile data server 116 generates its own short-term authentication key pair, also using the activation password. The mobile data server 116 also generates its own long-term encryption key pair. Using the public keys generated by the device 102 and the activation password, the mobile data server 116 generates a master encryption key. The activation password provides the authentication necessary to trust the information exchanged. The mobile data

server's short-term public authentication key, long-term public encryption key, a key confirmation value calculated using the newly generated master encryption key, and a known string, are sent to the device 102.

**[0033]** The device 102 receives the information from the mobile data server 116 and generates the device's own master encryption key. With this master key the device 102 verifies the key confirmation value. For example, the key confirmation value could be the hash of the master key the known string, as agreed upon by the device 102 and the mobile data server 116. If the key confirmation value does not verify, the master key created by the device 102 is not trusted, and it is assumed that someone is trying to compromise the connection. If the master encryption key generated by the device 102 seems valid, the device 102 sends a final key confirmation value to the mobile data server 116. The mobile data server 116 receives the message, verifies the key confirmation value and marks the device 102 as ready to go. Therefore, it will be appreciated that a secure communications tunnel can be established between the requesting device 102 and the mobile data server 116, and therefore the CA 118, even before the activation process is completed.

**[0034]** At this point the user and the mobile data server have been verified and full data exchange can securely take place using the corresponding long-term encryption key as desired. Data exchange may comprise e-mail messages, hypertext transfer protocol (HTTP)-based traffic, such as extensible markup language (XML), wireless markup language (WML), or other forms of data. Accordingly, if the master encryption key confirmation succeeds, the activation process proceeds with further communication being encrypted as desired.

**[0035]** In step 212, the mobile data server 116 and device 102 exchange data to facilitate further communication between the device 102 and the communication network 104 as well as the backend servers 108. As part of this data exchange, the device 102 requests, and is assigned, a device certificate.

**[0036]** In step 212a, the device 102 creates a certificate request using a digital certificate protocol. In the present embodiment, the device 102 creates a certificate signing request (CSR) using the Public-Key Cryptography Standards No. 10 (PKCS10) protocol. The PKCS10 protocol is well known in the art and need not be described in detail. It was developed by RSA Laboratories and is described in a document titled "PKCS #10 v1.7: Certification Request Syntax Standard", dated May 26, 2000. Although PKCS10 is used to implement the CSR, any appropriate protocol may used, as will be appreciated by a person of ordinary skill in the art.

**[0037]** In accordance with the PKCS10 protocol, a CSR has the following syntax: PKCSReq CertificationRequest ::= SEQUENCE {

```
certificationRequestInfo SEQUENCE {
        version INTEGER,
        subject Name,
        subjectPublicKeyInfo SEQUENCE {
               algorithm AlgorithmIdentifier,
                subjectPublicKey BIT STRING
                }
        attributes [0] Attributes{ { CRIAttributes } }
        }
signatureAlgorithm AlgorithmIdentifier,
signature BIT STRING
 }
```

**[0038]** Version is a version number of the PKCS10 protocol. It is used for compatibility with future revisions. Subject is the name of the certificate subject. SubjectPublicKeyInfo contains information about the public key being certified. The information identifies the entity's public-key algorithm and any associated parameters.

**[0039]** The attributes are a collection of data providing additional information about the subject of the certificate. More information about attribute types is provided in PKCS No. 9, developed by RSA Laboratories and described in a document titled "PKCS #9 v2.0: Selected Object Classes and Attribute Types", dated February 25, 2000. Alternately, the attributes may be locally defined. In accordance with the present embodiment, the attributes are used to transmit the user's email address as well as a personal identification number (PIN) associated with the device 102 as part of the CSR. This act binds the two identifiers together.

**[0040]** In step 212b, the CSR is received by the mobile data server 116, which has a predefined certification authority (CA 118) associated with it. Often, the CA 118 is a third party such as VeriSign® or Entrust®, for example. However, the mobile data server 116 may also act as its own CA 118. In this manner, a company or organization could operate the CA 118.

**[0041]** In step 212c, the CSR is transmitted to the predefined CA 118 for certification. The CA 118 signs the CSR with its private key and the signed CSR becomes the device certificate. In step 212d, the device certificate is returned to the device 102 for future use, when required.

**[0042]** Once the device 102 has the device certificate at its disposal, the mobile data server 102 can use it to ensure that the device is allowed on the communication network 104. For example, if the user is fired or the device is compromised,

the CA 118 can revoke the device certificate.

**[0043]** In general, a server or user manually checks to see if a device certificate has been revoked. This can be accomplished either by checking a Certificate Revocation List (CRL) that is published by the CA 118 by making an Online Certificate Status Protocol (OCSP) request. Accordingly, in order to check the status of a device certificate the mobile data server 116 can periodically make OCSP requests or check the CA's CRL.

**[0044]** After determining that a certificate has been revoked, the mobile data server 116 can automatically send a Kill command to the device 102 to disable it. The use of the device certificate helps to reduce the chance of activating the Kill command on the wrong device.

**[0045]** Alternately, the mobile data server 116 could refrain from forwarding traffic to and/or from the device 102 in the event that the digital certificate has been revoked. Therefore, it also reduces the chance of having an unwanted device on the network.

**[0046]** Accordingly, it will be seen that the embodiment described above provides a relatively simple method for obtaining a device certificate for a wireless device. Moreover. The device certificate is obtained when before the device is provisioned on the communication network 104, thus limiting fraudulent use of the devices 102 and access to sensitive data on one or more of the backend servers 108.

**[0047]** Although the embodiment described describes a specific implementation, a person of ordinary skill in the art will appreciate that other embodiments may also be realized.

**[0048]** For example, in the embodiment described above, the activation request message is an email. However, other forms of messaging may also be used successfully. For example, a custom handshaking protocol may be implemented or an alternate messaging protocol, such as Short Messaging Service (SMS) may be used.

**[0049]** Further, although the previous embodiment describes using an email address to identify the user and a PIN to identify the device 102, other parameters may be used. For the user, sufficient information to uniquely identify him or her is desired. Therefore, a social insurance number may suffice. Other information like name, address, telephone number, employer and the like, or any combination thereof, may also be sufficient to identify the user as required.

**[0050]** Similarly, rather than use the PIN to identify the device 102, other information such as a serial number, a mobile identification number (MIN), or International Mobile Subscriber Identity (IMSI), for example, may be used. Such information may be used alone, or in combination, as required.

**[0051]** In the embodiments described above, the mobile data server 116 polls the CA 118 to determine the status of a device certificate. In an alternate embodiment, the CA 118 transmits a notification to the mobile data server 116 when the certificate is revoked. In such an embodiment, the CA 118 maintains a correlation between the mobile data server 116 and the device certificate when the CSR is submitted.

**[0052]** In all of the embodiments described above, generation of a device certificate is a dynamic operation that takes place during the activation of the device. A further benefit of this arranged is realized when the system administrator has established its own CA 118.

**[0053]** In this case, their own CA 118 can issue the device certificates. This feature increases the amount of trust the system administrator has in the device certificate process.

## Claims

1. A method for provisioning a device certificate on a device (102) configured to communicate wirelessly with a plurality of backend servers (108) via a communication network (104) having a mobile data server (116), the method comprising the steps of:

   initiating an activation request (206) to the mobile data server (116) for activating the device (102) on the communication network (104);
   during activation of the device (102), providing a device certificate request (212a) to the mobile data server (116) for the device (102), the device certificate request comprising at least a user identifier, a device identifier and a device public key, wherein the device certificate request is forwarded (212c) from the mobile data server (116) to a predefined certification authority (118); and
   receiving (212d) a device certificate from the predefined certification authority (118) in response to the device certificate request.

2. The method of claim 1, wherein the user identifier is an email address.

3. The method of claim 1 or claim 2, wherein the device identifier is a device personal identification number or a device serial number or a device International Mobile Subscriber Identity 'IMSI'.

4. The method of any of claims 1 to 3, wherein the device certificate request is in the form of a Public-Key Cryptography Standards No. 10 certificate signing request.

5. The method of any of claims 1 to 4, wherein the predefined certification authority is maintained by the mobile data server or is a third party certification authority or is maintained by an administrator of the mobile data server.

6. The method of any of claims 1 to 5, further comprising the step of establishing a secure communications tunnel between the device and the mobile data server before requesting the device certificate.

7. The method of claim 6, wherein the device and the mobile data server each generate and exchange a pair of public encryption keys.

8. The method of claim 7, wherein the device and the mobile data server each use the public encryption key pairs and a shared secret to generate and verify a master encryption key.

9. The method of claim 8, where in the shared secret is an authentication password.

10. A method for provisioning a device certificate on a device (102) configured to communicate wirelessly with a plurality of backend servers (108) via a communication network (104) comprising a mobile data server (116), the method comprising the steps of:

receiving an activation request (206) at the mobile data server 116 for activating the device (102) on the communication network (104);
during activation of the device (102), receiving a device certificate request at the mobile data server (212b) for the device, the device certificate request comprising at least a user identifier, a device identifier and a device public key; and
forwarding (212c) the device certificate request from the mobile data server (116) to a predefined certification authority (118), wherein a device certificate is forwarded (212d) from the predefined certification authority (118) to the device (102) in response to the device certificate request.

11. The method of claim 10, wherein the user identifier is an email address.

12. The method of claim 10 or claim 11, wherein the device identifier is a device personal identification number or a device serial number or a device International Mobile Subscriber Identity 'IMSI'.

13. The method of any of claims 10 to 12, wherein the device certificate request is in the form of a Public-Key Cryptography Standards No. 10 certificate signing request.

14. The method of any of claims 10 to 13, wherein the predefined certification authority is maintained by the mobile data server or is a third party certification authority or is maintained by an administrator of the mobile data server.

15. The method of any of claims 10 to 14, further comprising the step of establishing a secure communications tunnel between the device and the mobile data server before requesting the device certificate.

16. The method of claim 15, wherein the device and the mobile data server each generate and exchange a pair of public encryption keys.

17. The method of claim 16, wherein the device and the mobile data server each use the public encryption key pairs and a shared secret to generate and verify a master encryption key.

18. The method of claim 17, where in the shared secret is an authentication password.

19. A wireless communication device (102) comprising:

means for initiating an activation request to a mobile data server (116) for activating the device (102) on a communication network (104);
means for providing a device certificate request (212a) to the mobile data server (116) for the device (102) during activation of the device (102), the device certificate request comprising at least a user identifier, a device

identifier and a device public key, wherein the device certificate request is forwarded (212c) from the mobile data server (116) to a predefined certification authority (118); and
means for receiving a device certificate (212d) from the predefined certification authority (118) in response to the device certificate request.

**20.** The device of claim 19, wherein the user identifier is an email address.

**21.** The device of claim 19 or 20, wherein the device identifier is a device personal identification number or is a device serial number or is a device International Mobile Subscriber Identity 'IMSI'.

**22.** The device of any of claims 19 to 21, wherein the device certificate request is in the form of a Public-Key Cryptography Standards No. 10 certificate signing request.

**23.** The device of any of claims 19 to 22, wherein the predefined certification authority is maintained by the mobile data server or is a third party certification authority or is maintained by an administrator of the mobile data server.

**24.** The device of any of claims 19 to 23, further configured to establish a secure communications tunnel with a mobile data server before requesting the device certificate.

**25.** The device of claim 24, wherein the device is configured to generate and exchange a pair of public encryption keys with the mobile data server.

**26.** The device of claim 25, wherein the device is configured to use the public encryption key pairs and a shared secret to generate and verify a master encryption key.

**27.** The device of claim 26, where in the shared secret is an authentication password.

**28.** A computer program product for provisioning a device certificate on a device (102) configured to communicate wirelessly with a plurality of backend servers (108) via a communication network (104) having a mobile data server (116), the computer program product comprising instructions which, when executed on a processor of the device (102), cause the device to implement the method of any one of claims 1 to 9 and/or the method of any of claims 10 to 18.

**Patentansprüche**

**1.** Verfahren zur Bereitstellung eines Gerätezertifikats für ein Gerät (102), das dazu konfiguriert ist, drahtlos mit mehreren nachgelagerten Servern (108) über ein Kommunikationsnetz (104) zu kommunizieren, das einen mobilen Datenserver (116) aufweist, mit den folgenden Schritten:

Initiieren einer Aktivierungsanfrage (206) an den mobilen Datenserver (116) zum Aktivieren des Geräts (102) im Kommunikationsnetz (104);
während der Aktivierung des Geräts (102), Senden einer Gerätezertifikatsanfrage (212a) an den mobilen Datenserver (116) für das Gerät (102), wobei die Gerätezertifikatsanfrage zumindest eine Benutzerkennung, eine Gerätekennung und einen öffentlich zugänglichen Geräteschlüssel umfasst, wobei die Gerätezertifikatsanfrage vom mobilen Datenserver (116) an eine vordefinierte Zertifizierungsstelle (118) gesendet wird und Empfangen (212d) eines Gerätezertifikats von der vordefinierten Zertifizierungsstelle (118) als Antwort auf die Gerätezertifikatsanfrage.

**2.** Verfahren nach Anspruch 1, wobei die Benutzerkennung eine E-Mail-Adresse ist.

**3.** Verfahren nach Anspruch 1 oder Anspruch 2, wobei die Gerätekennung eine persönliche Geräteidentifizierungsnummer oder eine Geräteseriennummer oder eine internationale Mobilfunk-Teilnehmer-Geräteidentität (device International Mobile Subscriber Identity) 'IMSI' ist.

**4.** Verfahren nach irgendeinem der Ansprüche 1 bis 3, wobei die Gerätezertifikatsanfrage in Form einer Asymmetrische-Kryptografie-Normen-Nr.-10-Zertifikatsunterschriftsanfrage vorliegt.

**5.** Verfahren nach irgendeinem der Ansprüche 1 bis 4, wobei die vordefinierte Zertifizierungsstelle vom mobilen Da-

tenserver geführt wird oder eine Anerkannte-Stelle-Zertifizierungsbehörde ist oder von einem Administrator des mobilen Datenservers geführt wird.

6. Verfahren nach irgendeinem der Ansprüche 1 bis 5, weiterhin mit dem Schritt des Herstellens eines sicheren Kommunikationstunnels zwischen dem Gerät und dem mobilen Datenserver vor dem Beantragen des Gerätezertifikats.

7. Verfahren nach Anspruch 6, wobei das Gerät und der mobile Datenserver jeweils ein Paar öffentlich zugänglicher Verschlüsselungscodes erzeugen und austauschen.

8. Verfahren nach Anspruch 7, wobei das Gerät und der mobile Datenserver jeweils die öffentlich zugänglichen Verschlüsselungscodepaare und ein geteiltes Geheimnis verwenden, um einen Master-Verschlüsselungscode zu erzeugen und zu verifizieren.

9. Verfahren nach Anspruch 8, wobei das geteilte Geheimnis ein Authentifizierungskennwort ist.

10. Verfahren zur Bereitstellung eines Gerätezertifikats für ein Gerät (102), das dazu konfiguriert ist, drahtlos mit mehreren nachgelagerten Servern (108) über ein Kommunikationsnetz (104) zu kommunizieren, das einen mobilen Datenserver (116) aufweist, mit den folgenden Schritten:

    Empfangen einer Aktivierungsanfrage (206) am mobilen Datenserver (116) zum Aktivieren des Geräts (102) im Kommunikationsnetz (104);
    während der Aktivierung des Geräts (102), Empfangen einer Gerätezertifikatsanfrage am mobilen Datenserver (212b) für das Gerät, wobei die Gerätezertifikatsanfrage zumindest eine Benutzerkennung, eine Gerätekennung und einen öffentlich zugänglichen Geräteschlüssel umfasst, und
    Weiterleiten (212c) der Gerätezertifikatsanfrage vom mobilen Datenserver (116) an eine vordefinierte Zertifizierungsstelle (118), wobei ein Gerätezertifikat von der vordefinierten Zertifizierungsstelle (118) an das Gerät (102) als Antwort auf die Gerätezertifikatsanfrage gesendet wird (212d).

11. Verfahren nach Anspruch 10, wobei die Benutzerkennung eine E-Mail-Adresse ist.

12. Verfahren nach Anspruch 10 oder Anspruch 11, wobei die Gerätekennung eine persönliche Geräteidentifizierungsnummer oder eine Geräteseriennummer oder eine internationale Mobilfunk-Teilnehmer-Geräteidentität (device International Mobile Subscriber Identity) 'IMSI' ist.

13. Verfahren nach irgendeinem der Ansprüche 10 bis 12, wobei die Gerätezertifikatsanfrage in Form einer Asymmetrische-Kryptografie-Normen-Nr.-10-Zertifikatsunterschriftsanfrage vorliegt.

14. Verfahren nach irgendeinem der Ansprüche 10 bis 13, wobei die vordefinierte Zertifizierungsstelle vom mobilen Datenserver geführt wird oder eine Anerkannte-Stelle-Zertifizierungsbehörde ist oder von einem Administrator des mobilen Datenservers geführt wird.

15. Verfahren nach irgendeinem der Ansprüche 10 bis 14, weiterhin mit dem Schritt des Herstellens eines sicheren Kommunikationstunnels zwischen dem Gerät und dem mobilen Datenserver vor dem Beantragen des Gerätezertifikats.

16. Verfahren nach Anspruch 15, wobei das Gerät und der mobile Datenserver jeweils ein Paar öffentlich zugänglicher Verschlüsselungscodes erzeugen und austauschen.

17. Verfahren nach Anspruch 16, wobei das Gerät und der mobile Datenserver jeweils die öffentlich zugänglichen Verschlüsselungscodepaare und ein geteiltes Geheimnis verwenden, um einen Master-Verschlüsselungscode zu erzeugen und zu verifizieren.

18. Verfahren nach Anspruch 17, wobei das geteilte Geheimnis ein Authentifizierungskennwort ist.

19. Drahtlos-Kommunikationsgerät (102) mit:

    Mitteln zum Initiieren einer Aktivierungsanfrage an einen mobilen Datenserver (116) zum Aktivieren des Geräts (102) in einem Kommunikationsnetz (104);

Mitteln zum Senden einer Gerätezertifikatsanfrage (212a) an den mobilen Datenserver (116) für das Gerät (102) während der Aktivierung des Geräts (102), wobei die Gerätezertifikatsanfrage zumindest eine Benutzerkennung, eine Gerätekennung und einen öffentlich zugänglichen Geräteschlüssel umfasst, wobei die Gerätezertifikatsanfrage vom mobilen Datenserver (116) an eine vordefinierte Zertifizierungsstelle (118) gesendet wird (212c); und
Mitteln zum Empfangen eines Gerätezertifikats (212d) von der vordefinierten Zertifizierungsstelle (118) als Antwort auf die Gerätezertifikatsanfrage.

**20.** Gerät nach Anspruch 19, wobei die Benutzerkennung eine E-Mail-Adresse ist.

**21.** Gerät nach Anspruch 19 oder 20, wobei die Gerätekennung eine persönliche Geräteidentifizierungsnummer oder eine Geräteseriennummer oder eine internationale Mobilfunk-Teilnehmer-Geräteidentität (device International Mobile Subscriber Identity) 'IMSI' ist.

**22.** Gerät nach irgendeinem der Ansprüche 19 bis 21, wobei die Gerätezertifikatsanfrage in Form einer Asymmetrische-Kryptografie-Normen-Nr.-10-Zertifikatsunterschriftsanfrage vorliegt.

**23.** Gerät nach irgendeinem der Ansprüche 19 bis 22, wobei die vordefinierte Zertifizierungsstelle vom mobilen Datenserver geführt wird oder eine Anerkannte-Stelle-Zertifizierungsbehörde ist oder von einem Administrator des mobilen Datenservers geführt wird.

**24.** Gerät nach irgendeinem der Ansprüche 19 bis 23, das weiterhin dazu konfiguriert ist, vor dem Beantragen des Gerätezertifikats einen sicheren Kommunikationstunnel mit einem mobilen Datenserver herzustellen.

**25.** Gerät nach Anspruch 24, wobei das Gerät dazu konfiguriert ist, mit dem mobilen Datenserver ein Paar öffentlich zugänglicher Verschlüsselungscodes zu erzeugen und auszutauschen.

**26.** Gerät nach Anspruch 25, wobei das Gerät dazu konfiguriert ist, die öffentlich zugänglichen Verschlüsselungscodepaare und ein geteiltes Geheimnis zu verwenden, um einen Master-Verschlüsselungscode zu erzeugen und zu verifizieren.

**27.** Gerät nach Anspruch 26, wobei das geteilte Geheimnis ein Authentifizierungskennwort ist.

**28.** Computerprogrammprodukt zur Bereitstellung eines Gerätezertifikats für ein Gerät (102), das dazu konfiguriert ist, drahtlos mit mehreren nachgelagerten Servern (108) über ein Kommunikationsnetz (104) zu kommunizieren, das einen mobilen Datenserver (116) aufweist, wobei das Computerprogrammprodukt Anweisungen umfasst, die, wenn sie auf einem Prozessor des Geräts (102) ausgeführt werden, das Gerät veranlassen, das Verfahren nach irgendeinem der Ansprüche 1 bis 9 und/oder das Verfahren nach irgendeinem der Ansprüche 10 bis 18 umzusetzen.

**Revendications**

**1.** Procédé d'approvisionnement d'un certificat de dispositif sur un dispositif (102) configuré pour communiquer de manière non filaire avec une pluralité de serveurs dorsaux (108) au moyen d'un réseau de communication (104) ayant un serveur de données mobile (116), le procédé comprenant les étapes qui consistent :

à initier une demande d'activation (206) au serveur de données mobile (116) pour activer le dispositif (102) sur le réseau de communication (104) ;
durant l'activation du dispositif (102), à fournir une demande (212a) de certificat de dispositif au serveur de données mobile (116) pour le dispositif (102), la demande de certificat de dispositif comprenant au moins un identifiant d'utilisateur, un identifiant de dispositif et une clé publique de dispositif, où la demande de certificat de dispositif est transmise (212c) du serveur de données mobile (116) à une autorité de certification prédéfinie (118) ; et
à recevoir (212d) un certificat de dispositif de l'autorité de certification prédéfinie (118) en réponse à la demande de certificat de dispositif.

**2.** Procédé de la revendication 1, où l'identifiant d'utilisateur est une adresse de courrier électronique.

3. Procédé de la revendication 1 ou de la revendication 2, où l'identifiant de dispositif est un numéro d'identification personnel ou un numéro de série de dispositif ou une identité internationale de l'abonné mobile "IMSI" de dispositif.

4. Procédé de l'une des revendications 1 à 3, où la demande de certificat de dispositif se trouve sous forme de demande d'attribution de certificat N°10 selon les normes de cryptographie à clé publique.

5. Procédé de l'une des revendications 1 à 4, où l'autorité de certification prédéfinie est maintenue par le serveur de données mobile ou est une autorité de certification tierce ou est maintenue par un administrateur du serveur de données mobile.

6. Procédé de l'une des revendications 1 à 5, comprenant en outre l'étape qui consiste à établir un tunnel de communications sécurisé entre le dispositif et le serveur de données mobile avant de demander le certificat de dispositif.

7. Procédé de la revendication 6, où le dispositif et le serveur de données mobile génèrent chacun et s'échangent une paire de clés de cryptage publiques.

8. Procédé de la revendication 7, où le dispositif et le serveur de données mobile utilise chacun les paires de clés de cryptage publiques et un secret partagé pour générer et vérifier une clé de cryptage maîtresse.

9. Procédé de la revendication 8, où dans le secret partagé se trouve un mot de passe d'authentification.

10. Procédé d'approvisionnement d'un certificat de dispositif sur un dispositif (102) configuré pour communiquer de manière non filaire avec une pluralité de serveurs dorsaux (108) au moyen d'un réseau de communication (104) comprenant un serveur de données mobile (116), le procédé comprenant les étapes qui consistent :

    à recevoir une demande d'activation (206) au serveur de données mobile (116) pour activer le dispositif (102) sur le réseau de communication (104) ;
    durant l'activation du dispositif (102), à recevoir une demande de certificat de dispositif au serveur de données mobile (212b) pour le dispositif, la demande de certificat de dispositif comprenant au moins un identifiant d'utilisateur, un identifiant de dispositif et une clé publique de dispositif ; et
    à transmettre (212c) la demande de certificat de dispositif depuis le serveur de données mobile (116) à une autorité de certification prédéfinie (118), où un certificat de dispositif est transmis (212d) de l'autorité de certification prédéfinie (118) au dispositif (102) en réponse à la demande de certificat de dispositif.

11. Procédé de la revendication 10, où l'identifiant d'utilisateur est une adresse de courrier électronique.

12. Procédé de la revendication 10 ou de la revendication 11, où l'identifiant de dispositif est un numéro d'identification personnel de dispositif ou un numéro de série de dispositif ou une identité internationale de l'abonné mobile "IMSI" de dispositif.

13. Procédé de l'une des revendications 10 à 12, où la demande de certificat de dispositif est sous forme de demande d'attribution de certificat N°.10 selon les normes de cryptographie à clé publique.

14. Procédé de l'une des revendications 10 à 13, où l'autorité de certification prédéfinie est maintenue par le serveur de données mobile ou est une autorité de certification tierce ou est maintenue par un administrateur du serveur de données mobile.

15. Procédé de l'une des revendications 10 à 14, comprenant en outre l'étape qui consiste à établir un tunnel de communications sécurisé entre le dispositif et le serveur de données mobile avant de demander le certificat de dispositif.

16. Procédé de la revendication 15, où le dispositif et le serveur de données mobile génèrent chacun et s'échangent une paire de clés de cryptage publiques.

17. Procédé de la revendication 16, où le dispositif et le serveur de données mobile utilise chacun les paires de clés de cryptage publiques et un secret partagé pour générer et vérifier une clé de cryptage maîtresse.

18. Procédé de la revendication 17, où dans le secret partagé se trouve un mot de passe d'authentification.

**19.** Dispositif de communication sans fil (102) comprenant :

un moyen destiné à initier une demande d'activation à un serveur de données mobile (116) pour activer le dispositif (102) sur un réseau de communication (104) ;

un moyen destiné à fournir une demande de certificat (212a) de dispositif au serveur de données mobile (116) pour le dispositif (102) durant l'activation du dispositif (102), la demande de certificat de dispositif comprenant au moins un identifiant d'utilisateur, un identifiant de dispositif et une clé publique de dispositif, où la demande de certificat de dispositif est transmise (212c) du serveur de données mobile (116) à une autorité de certification prédéfinie (118) ; et

un moyen destiné à recevoir un certificat de dispositif (212d) de l'autorité de certification prédéfinie (118) en réponse à la demande de certificat de dispositif.

**20.** Dispositif de la revendication 19, où l'identifiant d'utilisateur est une adresse de courrier électronique.

**21.** Procédé des revendications 19 ou 20, où l'identifiant de dispositif est un numéro d'identification personnel de dispositif ou un numéro de série de dispositif ou est une identité internationale de l'abonné mobile "IMSI" de dispositif.

**22.** Procédé de l'une des revendications 19 à 21, où la demande de certificat de dispositif est sous forme de demande d'attribution de certificat N°.10 selon les normes de cryptographie à clé publique.

**23.** Procédé de l'une des revendications 19 à 22, où l'autorité de certification prédéfinie est maintenue par le serveur de données mobile ou est une autorité de certification tierce ou est maintenue par un administrateur du serveur de données mobile.

**24.** Procédé de l'une des revendications 19 à 23, configuré en outre pour établir un tunnel de communications sécurisé avec un serveur de données mobile avant de demander le certificat de dispositif.

**25.** Procédé de la revendication 24, où le dispositif est configuré pour générer et échanger une paire de clés de cryptage publiques avec le serveur de données mobile.

**26.** Procédé de la revendication 25, où le dispositif est configuré pour utiliser les paires de clés de cryptage publiques et un secret partagé pour générer et vérifier une clé de cryptage maîtresse.

**27.** Procédé de la revendication 26, où dans le secret partage se trouve un mot de passe d'authentification.

**28.** Produit de programme informatique pour approvisionner un certificat de dispositif sur un dispositif (102) configuré pour communiquer de manière non filaire avec une pluralité de serveurs dorsaux (108) au moyen d'un réseau de communication (104) ayant un serveur de données mobile (116), le produit de programme informatique comprenant des instructions qui, lorsqu'elles sont exécutées sur un processeur du dispositif (102), amènent le dispositif à mettre en oeuvre le procédé de l'une quelconque des revendications 1 à 9 et/ou le procédé de l'une des revendications 10 à 18.

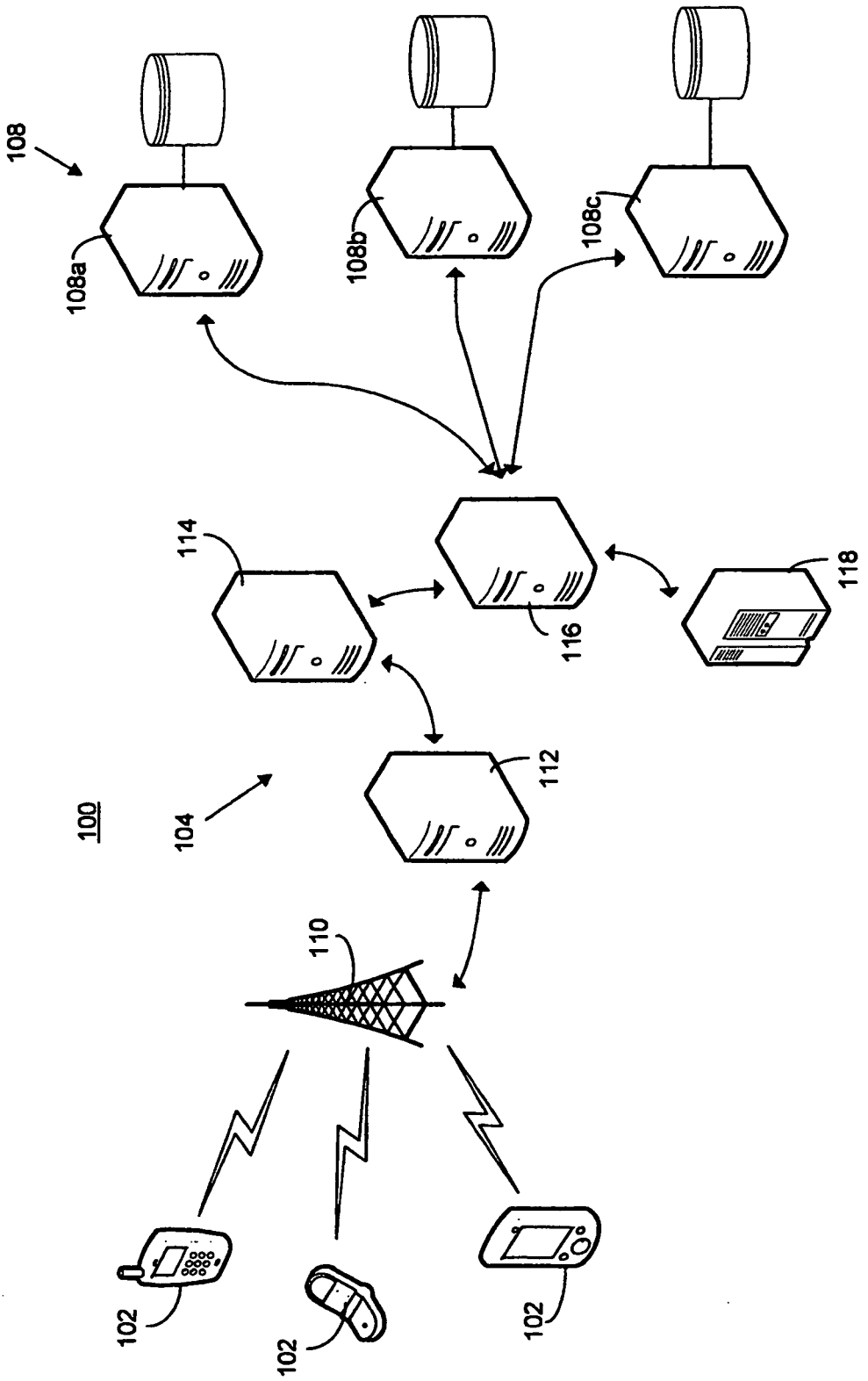



Figure 1

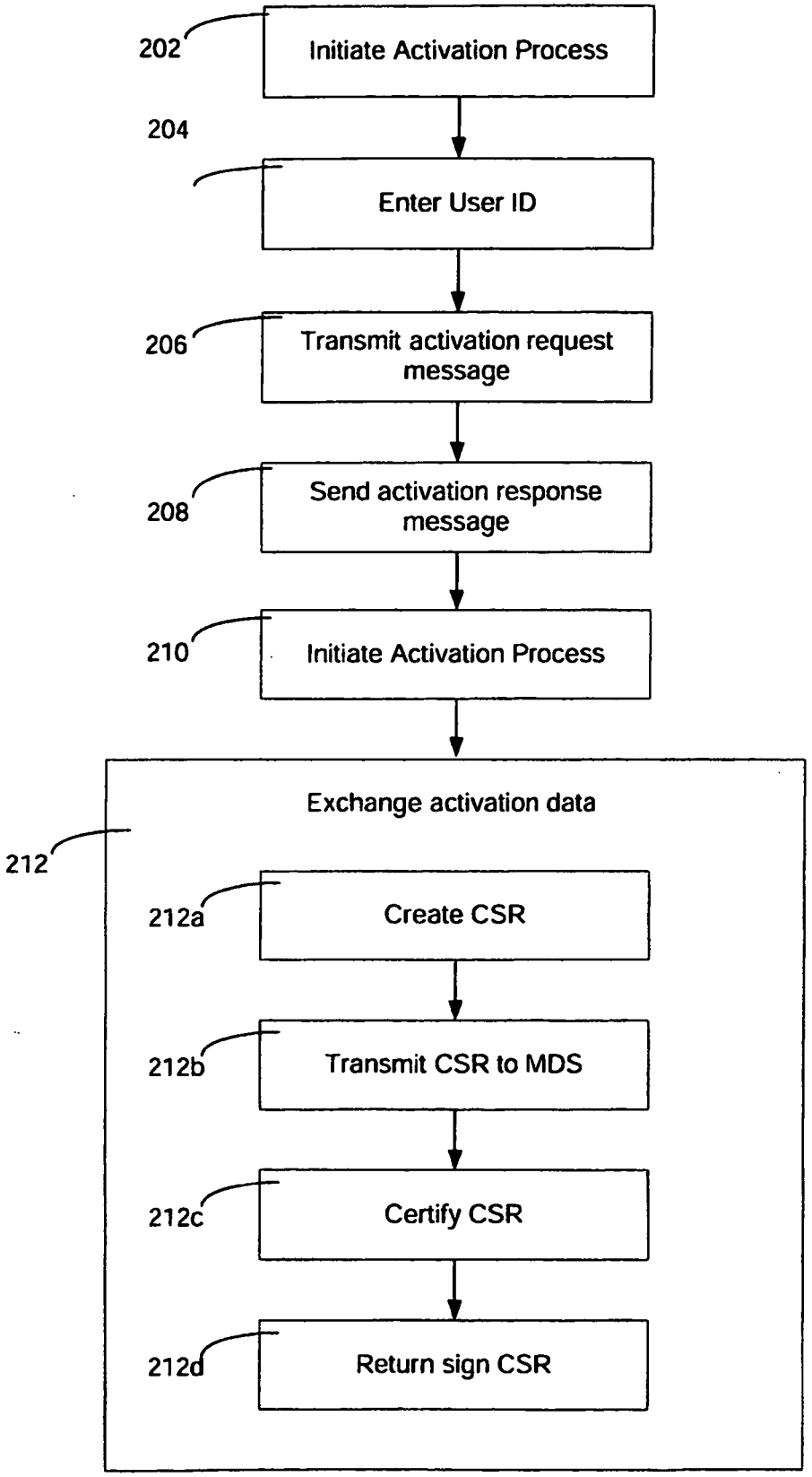

202
Initiate Activation Process
204
Enter User ID
206
Transmit activation request message
208
Send activation response message
210
Initiate Activation Process
212
Exchange activation data
212a
Create CSR
212b
Transmit CSR to MDS
212c
Certify CSR
212d
Return sign CSR

Figure 2

200

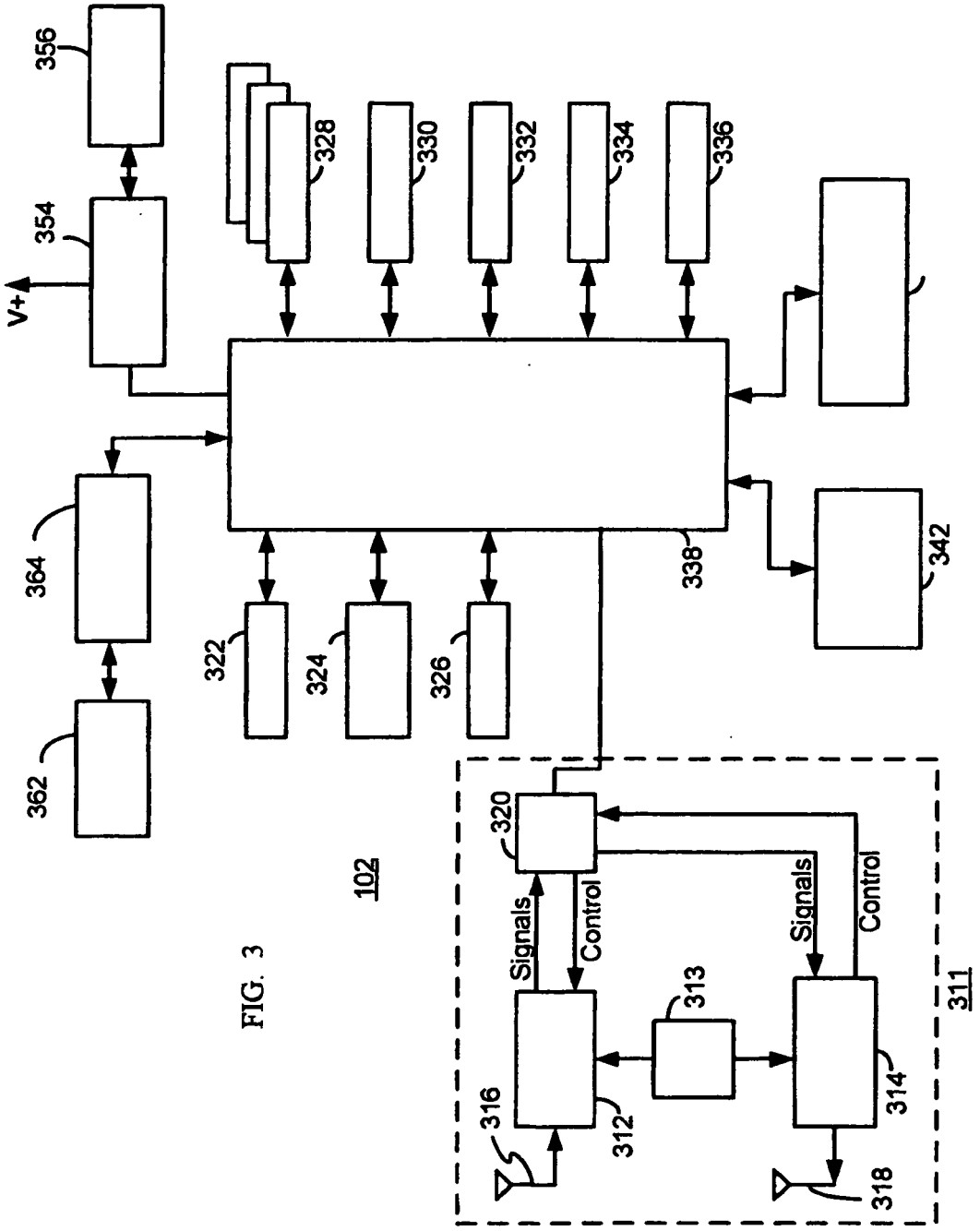

356
354
V+
328
330
332
334
336
364
362
322
324
326
338
342
102
320
Signals
Control
Signals
Control
313
316
312
314
318
311

FIG. 3

## REFERENCES CITED IN THE DESCRIPTION

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

### Patent documents cited in the description


- US 002315 A, Tet Hin Yeap **[0007]**
- US 20050287990 A **[0008]**
- US 09395405 A **[0031]**